

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri**FILED**

OCT 06 2020

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

INFORMATION ASSOCIATED WITH ACCOUNT: 1209650337
THAT IS STORED AT PREMISES CONTROLLED BY PINGER, INC

Case No. 4: 20 MJ 7277 SPM

) SIGNED AND SUBMITTED TO THE COURT FOR
) FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Mark Leone, a federal law enforcement officer or an attorney for the government,
request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or
property (*identify the person or describe the property to be searched and give its location*):

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed (*identify the
person or describe the property to be seized*):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

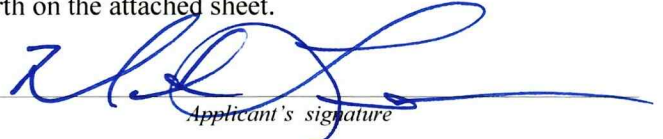
Code Section - Offense Description

18 USC 875 - Interstate communications

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing
is true and correct.

Mark Leone, Task Force Officer

*Printed name and title*Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedures
4.1 and 41.Date: 10/06/2020*Judge's signature*City and state: St. Louis, MO

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: Colleen C. Lang

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF:

INFORMATION ASSOCIATED WITH
ACCOUNT: 1209650337 THAT IS
STORED AT PREMISES CONTROLLED
BY **PINGER, INC.**

No. 4:20 MJ 7277 SPM

SIGNED AND SUBMITTED TO THE
COURT FOR FILING BY RELIABLE
ELECTRONIC MEANS

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, **Mark Leone**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by **PINGER, INC** (hereinafter the Provider), a cross-platform communication application publisher and developer headquartered at **97 South 2nd Street, Suite 210, San Jose, California 95113**. The information to be searched is described in the following paragraphs and in Attachment A. The requested warrant would require the Provider to disclose to the United States and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications as further described in Attachment B.

2. I am a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) and have been since February 2019, I have been a police officer for 18 years, with 13 years of

investigative experience as a detective. I am currently assigned to the St. Louis Field Office of the FBI, assigned to full-time investigations of specifically involving counterterrorism and other violent crime matters. Through my training and experience as a Police Officer and Task Force Officer, I am familiar with investigations involving individuals who use electronic means to threaten, harass, and intimidate others, including the execution of search warrants on computers, email accounts, telecommunication devices and other forms of electronic media.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of **Title 18 of the United States Code, Section 875** have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

LOCATION TO BE SEARCHED

4. This warrant applies to information associated with **ACCOUNT: 1209650337** that is stored at premises owned, maintained, controlled, or operated by **PINGER**, a company headquartered at **97 South 2nd Street, Suite 210, San Jose, California 95113**.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).]

BACKGROUND CONCERNING PINGER

6. Pinger is an application developer headquartered in San Jose, California. Pinger develops and publishes cross-platform communication applications that can be installed on Android and iOS devices or accessed using a desktop computer. Several Pinger applications allow for messaging, calling, and communication management tools. All communications are made utilizing the user's wi-fi, data, or cellular connection.

7. According to the Pinger Law Enforcement Guidelines, Pinger collects and stores user records such as Basic Subscriber Information (BSI), Detailed Message Logs (DML), Message Content (MC) and Internet Protocol Address Logs (IP Logs). Pinger is not a wireless carrier, and it does not have any cell site records or similar data that a wireless carrier would have. The information collected varies based on the Pinger application and device being used.

8. Pinger provides BSI in the form of a Pinger Customer Information Sheet (PCIS). Information within the PCIS is provided by the user, the user's operating system, or Pinger. Since Pinger is an application developer and not a Competitive Local Exchange Carrier (CLEC), information provided by the subscriber may not reflect the subscriber's true identity or real contact information. If available, the PCIS may include: Pinger phone number, Pinger account ID, Pinger application, IP address at account creation, Device information, Name, Pinger username, Third-party email address, Registered phone number

9. Pinger captures Detailed Message Logs (DMLs) about messages (SMS and MMS) that are sent from a Pinger number or to a Pinger number. These records will show the Date/Time that a message was received/sent, From Number, and To Number(s).

10. Pinger also records Message Content (MC) which captures the user's stored message communications (SMS and MMS). MC will include the aforementioned DMLs with the content of the user's communication. Pinger will only disclose message content in accordance with the Electronic Communications Privacy Act, [18 U.S.C. § 2703](#).

11. Pinger also maintains records concerning Internet Protocol Address Logs (IP Logs) which capture the user's internet protocol addresses as they are reported from the user's operating system. These records will show basic IP Addresses and the Date/Time they were captured to Pinger's servers.

PROBABLE CAUSE

12. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from victims and witness statements and records. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have been directly involved in this investigation since July of 2020. Currently, the primary target of this investigation is the unknown actor possessing the **Pinger Account: 1209650337**. The victim in this case, an elected official, received a threat of rape and murder to her personally owned mobile phone. The investigation revealed that the message was sent through a text message application that allows the sender the ability to "spoof" or imitate another phone number. This provided anonymity for the sender by masking the identity of the actual phone number from which the message was sent. By "spoofing" the number, this act lends credence to the likelihood that this was a premeditated and malicious act. Pinger captured the IP address and "Google Play Services ID" used to download the text message application. The records being sought in this warrant would confirm the account used to

send the threat, the content of the text message threat and link both the download and usage of the application to a specific device through the unique Google Play Service ID for Android (GPS ADID) that was captured by Pinger. A separate legal process is being sought to identify which mobile device is assigned to the "Google Play Service ID for Android" (hereafter "GPS ADID") in question. I have interviewed the victim and witnesses, as well as reviewed their records, in this investigation and can attest to the accuracy of the information contained in this affidavit.

13. On July 24, 2020, I was assigned to investigate an incident where St. Louis Mayor, L K, had received a threat to her life, by way of text message. The threat was initially investigated by members of the St. Louis Metropolitan Police Department before being transferred to the Federal Bureau of Investigation after it was determined that the unknown actor was likely a resident of Flushing, New York. The facts of the investigation are as follows:

a. On Saturday, June 27, 2020 at approximately 9:18pm (CST), L K (identified as LK hereon), Mayor of the City of St. Louis, received a text message to her personal cell phone that reads as follows:

"Hello
I'm parked outside you house
Should I come in and rape you
Maybe cut your throat
Would be nice
ave cute"

b. LK was at her home, located at Avenue, St. Louis, Missouri at the time the threat was received.

c. Caller ID indicated that the message was sent from phone number: 562-546-3931.

d. LK did not recognize the number and call/text history of her phone revealed no previous communication with that number in the past.

e. Due to the nature of the threat, several exigent circumstance requests were filed at that time.

f. The phone number 562-546-3931 was eventually identified as a “spoof number” registered to Bandwidth.com.

g. Bandwidth.com is in partnership with Pinger, Inc.

h. Pinger is an application developer headquartered in San Jose, California. Pinger develops and publishes cross-platform communication applications that can be installed on Android and iOS devices or accessed using a desktop computer. Several Pinger applications allow for messaging, calling, and communication management tools. All communications are made utilizing the user’s wi-fi, data, or cellular connection.

i. Pinger, Inc provided the user information with regards to the text threat. Some of the information (username, email, telephone number) is not required to be verified and can be manipulated, falsified or in some instances, left blank by the user. However, the IP address and Google Play Services ID for Android were captured.

j. The IP address was identified as being serviced by Cellco Partnership d/b/a Verizon Wireless.

k. Verizon Wireless identified the account customer as:

Customer ID: 255728407

Darwin Fuentes

[REDACTED]
Flushing, NY 11367

212-[REDACTED]

supapwned@gmail.com

l. Additionally, the mobile telephone number “212- [REDACTED]” has been confirmed through legal process to T-Mobile, as being registered to Darwin Fuentes, resident of Flushing, New York.

m. On Wednesday, July 15, 2020, Special Agent Sarah Bernal of the Federal Bureau of Investigation – NY Field Office, interviewed Darwin Fuentes at his home, during which, Fuentes consented to a search of his cell phone.

n. It is worth mention that Fuentes lives alone and used a “biometric” fingerprint to grant access to his phone.

o. Search history on the cell phone revealed that Fuentes searched these phrases: “send texts anonymously,” “send an anonymous text message,” and “St. Louis mayor reads names and addresses of protesters who want to defund the police” on June 27, 2020, the same day that the text threat was sent to LK.

p. Fuentes denied ever using an application named, “anonymoustext.com,” which was in his Internet search history. Fuentes went on to say that if he would have sent an anonymous text, he would have used the “Text Free” application he has used in the past. “Text Free” is an application supported by Pinger, Inc and the same developer of the application used to send the text threat in this case.

q. With regards to the text threat content, Fuentes said he did not recall sending the text, but admits that he does use the word “cute” as a closing signature when sending text messages.

r. Fuentes later provided SA Bernal with a copy of his T-Mobile billing

statement that indicates he has three devices on his account ([REDACTED] 38877) with the telephone numbers; 212-[REDACTED], 212-470-[REDACTED] and 917-600-[REDACTED]

s. It is unknown which device was used to send the text threat.

t. On July 24, 2020, I interviewed LK, who allowed me to view the text message threat sent to personal mobile phone.

u. When asked, LK stated she does not know Darwin Fuentes.

v. It is worth mention that at the time LK received the text message, the City of St. Louis had been experiencing nightly protests, which on occasion devolved into violence, rioting and looting.

w. As a result of receiving this text message, LK and her husband were placed in fear for their lives and fled their home the next day (06/28/2020).

x. As of the date of the interview (07/24/2020), LK and her husband have not returned to live in their residence.

y. This warrant is seeking to obtain the message content and identify the person(s) and device(s) associated with aforementioned Pinger account.

z. Separate legal processes have been served to both Google to identify the device associated with the “Google Play Service ID for Android” (GPS ADID) and another, to T-Mobile to identify the devices (make/model/serial number of the mobile telephone) assigned to the corresponding phone numbers.

aa. Therefore, the evidence obtained through this search warrant, in conjunction with the legal processes being served to Google and T-Mobile, will confirm the content of the text message threat, the Google Play Service account (that is device

specific) used to download and send the message to a specific device and finally to the owner of the device in question.

bb. A preservation requested has already been served to Pinger to retain the records associated with the account in question.

cc. Lastly, Pinger account 1209650337 has been confirmed by a Pinger representative to still be an active account and present in their system.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

14. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require the Provider to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

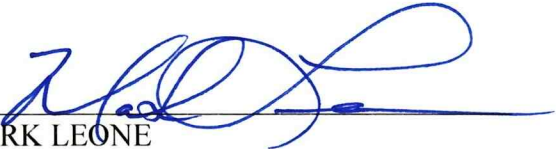
CONCLUSION

15. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on the Provider. Because the warrant will be served on the Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

16. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

17. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

I state under the penalty of perjury that the foregoing is true and correct.


MARK LEONE
Task Force Officer
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 6th day of October 2020.


SHIRLEY P. MENSAH
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **ACCOUNT 1209650337** that is stored at premises owned, maintained, controlled, or operated by **PINGER**, a company headquartered at **97 South 2nd Street, Suite 210, San Jose, California 95113**.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by PINGER

To the extent that the information described in Attachment A is within the possession, custody, or control of **PINGER**, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to **PINGER**, or have been preserved pursuant to a request made under [18 U.S.C. § 2703\(f\)](#), **PINGER** is required to disclose the following information, from **06/26/2020 to 06/28/2020**, to the United States for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- b. Message Content (MC), to include Detailed Message Logs (DML's), for text messages (SMS or MMS) conducted from 06/26/2020 to 06/28/2020.
- c. All Geo-location information
- d. The types of service utilized by the user;
- e. All records pertaining to communications between **PINGER** and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the United States within fourteen days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 875 involving an unknown actor since **06/27/2020**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

b. Message Content (MC), to include Detailed Message Logs (DML's), for text messages (SMS or MMS) conducted from 06/26/2020 to 06/28/2020.

c. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

d. All Geo-location information

e. The types of service utilized by the user;

f. All records pertaining to communications between the provider and any person regarding the account, including contacts with support services and records of actions taken.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS
PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **PINGER**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **PINGER**. The attached records consist of _____

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **PINGER**, and they were made by **PINGER** as a regular practice; and

b. such records were generated by **PINGER'S** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **PINGER** in a manner to ensure that they are true duplicates of the original records; and
2. the process or system is regularly verified by **PINGER**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

ate

Signature